Unclassified
Summer 2003
No. 82

Canadian Security Intelligence Service

Commentary

Reshaping Intelligence to Share with "Ourselves"

Gregory F. Treverton

Introduction

The world of intelligence was just starting to come to grips with the end of the Cold War when the September 11 terrorist attacks occurred. The collapse of the Soviet Union took away the threat by which all else was measured. Meanwhile, rapidly changing technology was blurring the distinction between strategic and tactical intelligence, and the explosion of global information networks was creating both opportunities and competition for national intelligence agencies. The end of the Soviet Union and the shrinking of "denied areas" in the world, plus the technological revolution, meant that intelligence was beginning to learn to cope with huge amounts of openly available information, but which mixed fact, fiction, fancy and disinformation.

Then September 11 struck. It made all too real an emerging threat, and created a sudden demand for an immediate response by intelligence—a response across not just levels of government in federal systems. The response also needed to cut across distinctions—law enforcement and intelligence, domestic and foreign, public and private—that were already coming into question. That response may be the hardest of all, for it requires intelligence not only to share information across nations, but to work at home with a range of government officials and private citizens who are newcomers to intelligence, to what it is, what it can do and what it cannot.

The size and technology of U.S. intelligence put it in a class by itself. Yet it is striking the extent to which countries that took intelligence seriously during the Cold War face fractals of the same challenge—whether those countries are former neutrals, NATO allies or former enemies. All have significant intelligence institutions, ones that for the most part were dominated by the military. All of them are asking how that capacity can be reshaped to cope with a new world and new threats, and do so without infringing too much on the liberties of their citizens. In that sense, the example of the United States can be instructive, and so, too, can the United States learn from the experiences of others.

The Cold War Legacy

During the high Cold War, there was a certain logic to the way U.S. intelligence was, and is, organized. It was structured by *source,* according to the different ways intelligence is collected—the National Security Agency (NSA) for intercepting signals, or SIGINT; the CIA's clandestine service for spying, or human intelligence (HUMINT) and the recently created National Imagery and Mapping Agency (NIMA) for imagery or IMINT. (In the special language of intelligence, everything not from a secret source is referred to as "open source.") These different "INTs," or "stovepipes" in the language of insiders, could each concentrate on the distinct contribution it made to understanding the over-arching target, the Soviet Union. In the process, though, the INTs became formidable baronies in their own right. Meanwhile, analysis was centralized in the CIA's Directorate of Intelligence (DI) but not monopolized there; it had competitors in the Defense Intelligence Agency (DIA), State's Bureau of Intelligence and Research (INR), and elsewhere around official Washington.

Now, however, the old structure just has to be wrong. No business would organize this way, so much has changed. During the Cold War, there was one pre-eminent target, the Soviet Union, a fairly narrow set of consumers—mostly political military officials in the U.S. government, and a limited amount of information, mostly from special sources "owned" by intelligence and deemed reliable. In the new environment, however, there are many targets and many consumers, along with torrents of information, most of it not "owned" by intelligence and of widely varying reliability—as anyone who surfs the Internet can testify.

The explosion of information means that policy officials will be more, not less, reliant on information brokers. If collection is easier, *selection* will be harder. The more open world is blurring the Cold War's distinction between collection and analysis. The best looker is not a spy-master, much less an impersonal satellite, but someone steeped in the substance at hand—in short, an analyst. Yet analysts now get rewarded for being generalists, not deep specialists, and in some areas, like economics, intelligence cannot compete with the private sector. Analysts are, though, cheap by comparison to satellites, and hiring more people from outside, even for brief tours, would deepen the intelligence community's expertise.

Puzzles versus Mysteries

Now, intelligence is in the information business, not just the secrets business, a sea-change for the profession. In the circumstances of the information age, it is time for the intelligence community to "split the franchise" between puzzles and mysteries. Puzzles have particular solutions, if only we had access to the necessary (secret) information. Puzzles were the intelligence community's stock-in-trade during the Cold War: how many missiles does the Soviet Union have? How accurate are they? What is Iraq's order of battle? The opposites of puzzles are "mysteries," questions that have no definitive answer even in principle. Will North Korea strike a new nuclear bargain? Will China's Communist Party cede domestic primacy? When and where will Al Qaida next attack? No one knows the answers to these questions. The mystery can only be illuminated; it cannot be "solved."

Today's tactical puzzles where secrets matter are both fewer and more varied than the Cold War's Soviet puzzles, but they retain their importance. For solving puzzles, analysts need to be close to the collectors of secrets. In a world of too much information, policy-makers will want to "pull" up what they need, not have information "pushed" upon them; they will want to pull up puzzle solutions when they need them, not receive a torrent of information whether they ask for it or not. Yet solving the puzzle is often important enough that getting policy officials to pay attention is not a problem.

Mysteries, such as where and how terrorists will next attack, are surely more abundant now, and the franchise of framing strategic mysteries is very different from puzzle-solving. For it, analysts need access to secrets, but their crucial partnerships are those with colleagues outside intelligence and outside government, in the academy and think-tank world, in non-governmental organizations (NGOs) and in the world of private business. Intelligence needs to be opened wide, not cosseted in

secret compartments. This franchise is based upon the recognition that intelligence's business is information, not secrets, and that its product is people (experts), not paper.

In a world where both structures and U.S. interests are up for grabs, policy-makers might be better served by intelligence brokers close at hand—down the hall, not out at the CIA in Virginia. This argues for blurring another of the Cold War's distinctions, that between policy and intelligence. There are some consistent alignments among targets, analysts, customers and collectors. In these circumstances, a firm would organize around lines of business, establishing a distributed network or a loose confederation in which different parts of intelligence would endeavour to build very close links to the customers each served. The existing Director of Central Intelligence (DCI) centers–for counter-terrorism, counter-narcotics, and the like–are a suggestive model. They organize around a problem or line of policy. Their limitation is that they primarily integrate *within* the world of intelligence, though they do provide a focal point for connecting to policy. And the distributed network would be "virtual," not bricks and mortar, because while some problems, like North Korea or terrorism, will be enduring, others will rise and recede quickly.

The Force of Cold War "Oppositions"

The Cold War legacy ran deeper than establishing distinctions between secrets and open information, analysts and collectors, and policy and intelligence. For good reasons, mostly associated with protecting the rights of citizens, the United States set up "oppositions" that also were not bad during the Cold War but set us up to fail now in the war on terrorism.

The first opposition is law enforcement versus intelligence. The two are very different worlds. Intelligence is oriented toward the future and seeks to inform policy makers. It lives in a blizzard of uncertainty where the "truth" will never be known for certain. Because intelligence strives above all to protect its sources and methods, intelligence officials want desperately to stay out of the chain of evidence so they will never have to testify in court. By contrast, law enforcement is not interested in policy. Rather, its business is the prosecution of cases. And law enforcement knows that if it is to make a case, it must be prepared to reveal something of how it knows what it knows.

The second is foreign versus domestic. When President Harry Truman created the CIA in 1946, he worried openly about a "Gestapo-like organization," and so the new agency was barred from both law enforcement and domestic activity. In the 1970s, it was literally true that the directors of the CIA and FBI didn't speak to one another. That state of affairs has improved, but still relations between the two are frayed. The National Security Agency is also barred from law enforcement and from domestic spying, so if the trail of conversations on which it is eavesdropping becomes "domestic"—that is, involves a U.S. citizen, corporation or even resident alien – the trail must end.

In the mid-1970s, Congress's first-ever inquiry into intelligence (which I served as a staffer), the Senate Select Committee on Intelligence Activities, headed by then-Sen. Frank Church, D-Idaho, investigated abuses of the rights of Americans. The most serious of those abuses, which included

the harassing of Martin Luther King along with many American religious and political groups, had emerged from COINTELPRO, a curious mixing by the FBI of law enforcement and intelligence ostensibly for domestic counter-intelligence purposes. Our response was to *raise* the walls between intelligence and law enforcement – for instance by creating a special court, the Federal Intelligence and Surveillance Court (FISC), to review applications for national security, as opposed to law enforcement, wiretaps and surveillance.

The third opposition is public versus private. During the Cold War, national security was a federal government monopoly. To be sure, private citizens and corporations were involved, but there was a neat correspondence between the threat as defined and the federal government's national security machinery that was developed to meet that threat. The war against terrorism and homeland security will be much less a federal government monopoly. Ordinary Americans and the economy are already suffering the inconvenience and higher business costs of much tighter security. And tragically, more ordinary Americans are likely to die – drawn involuntarily into the war against terrorism.

All three of these distinctions—between law enforcement and intelligence, foreign and domestic and public and private—were all too vividly on display before September 11. The investigation of the joint House-Senate committee looking into September 11 provided new details but did not change the basic story.[1] Sharing of information across the oppositions was ragged at best. Focused on law enforcement and constrained by the need to open a case, the FBI's pursuit of the antiterrorism mission was uneven. Blocked by the high walls protecting privacy, the FBI couldn't get into alleged 20th hijacker Zacarias Moussaoui's laptop until after the attacks.

For instance, the CIA apparently sent a cable, in August 2001, warning of two Osama Binladen associates who had entered the United States and two others who were expected to attempt entry. Apparently, the FBI did little with the information and also failed to share it with the Immigration and Naturalization Service until the INS had already admitted the other two into the country, on the grounds that the INS was not a "law enforcement" organization. No agency told the Federal Aviation Administration to be on the lookout for the four men, apparently because it, too, was not in the law enforcement business. And nobody told the airlines because they were private, not public.

Meanwhile, the suspected "twentieth hijacker," Zacarias Moussaoui, had been arrested on August 16 in Minneapolis for a visa violation. FBI agents at the field office suspected him of terrorism and sought, increasingly desperately, to search his laptop computer. They were frustrated in a debate with headquarters and the Justice Department about one of those walls between intelligence and law enforcement that had been raised during the 1970s, the FISC. Before FISC, presidents had claimed the prerogative of warrantless searches for national security purposes, so the court was a compromise between presidential discretion and civil liberties. Before September 11, however, by the FISC

[1] See http://www.fas.org/irp/congress/2002_rpt/index.html

standard, the "primary purpose" of any search had to be a suspected connection to a foreign power, and Moussaoui, who at that point had been connected only to the rebels in Chechnya, did not meet that standard.[2]

Sharing with "Ourselves"

The distinctions were not forced on the United States. Rather, for the most part, Americans chose them, and mostly for good reasons. In a very real sense, the CIA and FBI were meant to cooperate, but not *too* closely, lest the rights of Americans be violated. The rub is that the terrorist threat does not respect any of those distinctions. It bridges the old world of intelligence and the new. It is part of the old world because terrorists hardly advertise their plans, so traditional intelligence methods of spying and eavesdropping are critical. But it is a part of the new world because even the United States cannot fight the war on terrorism alone. Even if the United States improved its HUMINT dramatically, other nations and groups—including some that are not friends—would have more success against hard terrorist targets. The United States has disclosed that it is sharing intelligence with 24 nations that it had not cooperated with prior to the present war. These include Sudan, which would have been nothing more than a target before September 11.

The still harder challenge may be cooperating with "ourselves"—across the oppositions. Not only are there, by one count, 18,000 governmental entities involved in the war on terrorism in the United States, but there are many more if private players are added, not just corporations but NGOs as well, and almost none of them have security clearances. Not surprisingly, thus far intelligence-sharing has been very haphazard. After September 11, it turned out that there was information about possible nuclear threats to New York, information that no part of the federal government troubled to share with New York officials. At the other extreme, California's governor interpreted very skimpy information about threats to the state's bridges as a reason for public announcement and stepped-up protection.

Like Canada, the United States has begun the process of rethinking Cold War distinctions. Intelligence and law enforcement have been pushed toward each other, yet how far remains controversial. For instance, the 2001 USA Patriot Act made it easier to move information across the organizational divide. Before the law was enacted, any information that was before a federal grand jury could be shared with CIA analysts *only* with a court order. Thus, analysts might be denied access to information that was a critical puzzle piece in their effort to understand terrorist networks. Now, that information can be shared more easily. The act also loosened the FISC standard to permit covert searches if investigating the suspicion of a foreign connection was a "secondary purpose." The new law updated wiretapping authority to cope with a world of multiple, mobile cell phones, not just static, analog phones. In 2002, FBI director Robert Mueller relaxed rules that had restricted FBI agents from activities that are permitted to ordinary citizens, such as surfing the Internet or visiting churches and similar public places of interest.

---

[2] Philip Shenon, "Traces of Terror: The Terror Suspect," *New York Times,* July 7, 2002, p. A24.

In the autumn of 2002, Congress authorized a new Department of Homeland Security (DHS), with its own intelligence unit. That unit will have authority to both receive raw intelligence and task the intelligence collectors. It will need access to foreign intelligence and to the domestic material that emerges from law enforcement. It will not be simply a departmental intelligence operation like the State Department's Bureau of Intelligence and Research. Rather, it also should serve the broader set of officials, especially in the White House office, whose mandate is homeland security.

It will be focused on terrorism and oriented domestically. Of current institutions, the CIA and intelligence's Counterterrorism Center, which is located at the CIA, are, for legal reasons, aimed mostly abroad. Operators, not analysts, have dominated the Center. Before the DHS, remarkably, no agency systematically reviewed domestic information for intelligence and warning purposes—as opposed to law enforcement; the FBI has only expressed the intention to begin doing so.

The DHS intelligence capacity should link intelligence more tightly to warning. Getting warning too close to operations was a concern after the bombing of Pearl Harbor in 1941, but seems the right approach now. In the run-up to Pearl Harbor, Army and Navy intelligence had, apparently, been reluctant to sound the tocsin based on what was inevitably "iffy" evidence. They were close to their operational colleagues and thus knew that it was a costly nuisance for those operators to act on warning – for instance, putting the fleet to sea – if the warning turned out to be a false alarm.[3] The concern is fair, but now the warners (at the CIA, for instance) are so disconnected from those who must act that they are tempted to overwarn – a temptation in evidence in the summer of 2002. Moreover, the new assessment capacity will have lots of competition around town, hence lots of checks should its assessments appear to be tailored to suit the convenience of DHS operators.

The new unit also could provide additional incentive for the CIA and the FBI to communicate, in the form of another set of eyes looking at, and to, both, and trying to integrate information from both. It hardly would be decisive in producing easier communication between the two main agencies—there is too much history, not to mention constitutional concern. But the new intelligence unit would be a customer with a direct stake in the intersection of the information and analysis produced by the two.

The homeland security office instituted a stoplight chart of national warning, ranging from green through blue, yellow and orange, to red. The idea was based on twenty years of experience in Britain. It is a good one, but the United States lacks Britain's experience, so no one--not state and local officials, much less private citizens—knows yet what the colors mean. With time and experience, the DHS intelligence assessors could help the colors begin to acquire some meaning for public officials and private citizens alike.

---

[3] The classic study of the failure of warning at Pearl Harbor is Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford: Stanford University Press, 1962).

Rethinking "Domestic" Intelligence

The implications of the changed threat run well beyond organization, to what is collected, by whom and under what restrictions—very sensitive issues of domestic intelligence gathering. The September 11 terrorists not only trained in Afghanistan, they also used European cities like Hamburg, Germany, and Brixton, England, as staging areas where they could live, train and recruit in a protective environment. Similarly, they mixed easily in some areas of the United States, south Florida and southern California, or Buffalo, New York. The nation's need is not just to follow individuals, it is also to know what is being said on the streets and in the mosques of Brixton or Boston—it is doing what has heretofore been considered "foreign" intelligence domestically.

The terrorist threat takes us back to just the thicket that investigations of intelligence worried about a generation ago. Then, the investigations led to higher walls between intelligence and law enforcement. Now, shifting the culture of the FBI from law enforcement to prevention, as Director Mueller has called for, is a dramatic change, so dramatic that it may not be wise. In any case, it is the work of a generation, not a couple of years. Ultimately, if we require not just good law enforcement but good domestic intelligence, can the FBI do both? Former national security adviser Brent Scowcroft suggested creating a separate career track in the bureau for intelligence—a call that fell on stony ground. By tradition, law enforcement has been the bureau's dominant mission, and its internal pecking order has been dominated by special-agents-in-charge. Should the FBI be split into two agencies, one for law enforcement and the other for domestic intelligence?

If domestic intelligence is now an urgent need, should we create not just a Department of Homeland Security, but a home office—our version of MI-5, the British domestic intelligence service—as several members of Congress have suggested? Creating a new service would not solve the turf disputes born of overlapping missions—MI-5 and Britain's pre-eminent law enforcement agency, Scotland Yard, disputed for years which one would take the lead in dealing with the IRA terrorist threat to England. But, somewhat paradoxically, a separate U.S. domestic service might make for clearer lines of accountability than would making domestic intelligence the stepchild in a reshaped FBI.

And if domestic intelligence means not just tracking suspected terrorists but also monitoring the chatter in the mosques of Chicago or the strip malls of south Florida, how much risk are we prepared to run that rights of Americans, let alone non-Americans (who have far fewer), will be compromised? Finally, in the other direction, how does the public provide warning? Do people call local authorities, visit Web sites or offer anonymous tips? Should there be penalties for false calls or for tips that turn out to be score-settling? How should feedback be handled? Local authorities now complain routinely that they never hear what happens with information they provide to the FBI.

These questions lie ahead. Tomorrow's answers will not be the same as yesterday's, and it makes sense to take some time to frame those answers. But they will depend on assessments of the urgency of the terrorist threat, and thus where the nation feels it must strike the delicate balance between protecting its citizens and safeguarding their liberties.

Gregory F. Treverton is senior policy analyst at RAND and senior fellow at the Pacific Council on International Policy, a West Coast leadership forum. His latest book, *Reshaping National Intelligence for an Age of Information* is available from Cambridge University Press; http://www.cup.org

Commentary is a regular publication of the Research, Analysis and Production Branch of CSIS. Inquiries regarding submissions may be made to the Director General of the Research, Analysis and Production Branch at the following address: Box 9732, Stn. "T", Ottawa, Ont., K1G 4G4, or by fax at (613) 842-1312. Consult our World Wide Web site on the Internet for back issues of *Commentary*: http://www.csis-scrs.gc.ca

ISSN 1192-277X
Catalogue JS73-1/82

Et si le renseignement national ne signifie pas seulement traquer de présumés terroristes mais aussi écouter les bavardages dans les mosquées de Chicago ou les centres commerciaux du sud de la Floride, dans quelle mesure sommes-nous prêts à prendre le risque que les droits des Américains, sans parler de ceux des non-Américains (qui en ont beaucoup moins) soient compromis? Enfin, dans l'autre sens, comment le public donne-t-il l'alerte? Les gens appellent-ils les autorités locales, visitent-ils les sites Web ou donnent-ils des indices de façon anonyme? Devrait-il y avoir des sanctions pour les fausses alertes ou les indices qui finalement sont une forme de règlement de compte? Que faire de la question de la rétroaction? Les autorités locales se plaignent régulièrement de ne jamais entendre parler des informations qu'elles fournissent au FBI.

C'est à ces questions qu'il faut répondre. Les réponses de demain ne seront pas les mêmes que celles d'hier, et il est logique de prendre le temps de formuler ces réponses. Mais elles dépendront de l'évaluation de l'urgence de la menace terroriste et, en conséquence, de ce que la nation jugera être un juste milieu entre la protection de ses citoyens et la défense de leurs libertés.

Gregory F. Treverton est analyste principal de politiques à la RAND et membre supérieur du Pacific Council on International Policy, un forum de dirigeants de la côte Ouest. Son dernier livre, *Reshaping National Intelligence for an Age of Information*, est publié par Cambridge University Press; http://www.cup.org

Commentaire est publié régulièrement par la Direction de la recherche, de l'analyse et de la production du SCRS. Si vous avez des questions sur la teneur du document, veuillez vous adresser au directeur général de la Direction de la recherche, de l'analyse et de la production à l'adresse suivante : C.P. 9732, Succursale « T », Ottawa (Ontario), K1G 4G4; ou par télécopieur au (613) 842-1312. Consultez notre site Internet pour les numéros antérieurs de *Commentaire* : http://www.csis-scrs.gc.ca

ISSN 1192-277X
Catalogue JS73-1/82

encore ce que les couleurs signifient. Avec le temps et l'expérience, des analystes du renseignement du Département de la sécurité intérieure pourraient aider à mieux faire comprendre aux autorités publiques et aux simples citoyens ce que ces couleurs signifient.

Repenser le renseignement « national »

La nouvelle menace a des répercussions qui se font sentir bien au-delà de l'organisation relativement à ce qui est recueilli, par qui et à quelles conditions - autant de questions très sensibles concernant la collecte de renseignements au pays. Les terroristes du 11 septembre ne s'étaient pas seulement entraînés en Afghanistan. Ils avaient aussi utilisé des villes européennes telles que Hambourg, en Allemagne, et Brixton, en Angleterre, comme bases où ils pouvaient vivre, s'entraîner et recruter d'autres individus dans un milieu protégé. De même, ils s'intégraient facilement dans certaines régions des États-Unis, comme le sud de la Floride et de la Californie, ou Buffalo dans l'État de New York. Pour le pays, il n'est pas seulement nécessaire de suivre des individus. Il faut aussi savoir ce qui se dit dans la rue et dans les mosquées de Brixton ou de Boston. Il faut faire dans un contexte national ce qui jusqu'à présent était considéré comme des activités faisant partie du renseignement « étranger ».

La menace terroriste nous ramène aux écheveaux d'enquêtes qui étaient une source de préoccupation il y a une génération. Puis des murs plus hauts ont été érigés entre le renseignement et l'application de la loi. Maintenant, changer la culture du FBI pour passer de l'application de la loi à la prévention, comme le directeur Mueller l'a demandé, constitue un changement si radical qu'il n'est peut-être pas sage. Quoi qu'il en soit, c'est le travail de toute une génération, pas de deux ou trois années. En bout de ligne, s'il faut être efficace pas seulement en matière d'application de la loi mais aussi sur le plan du renseignement national, le FBI peut-il s'occuper des deux domaines? L'ancien conseiller en sécurité nationale, Brent Scowcroft, a proposé, mais en vain, de créer au FBI un cheminement de carrière distinct pour le renseignement. Traditionnellement, la mission principale du FBI a été l'application de la loi, et la hiérarchie interne du bureau a été dominée par des « special agents in charge » (agents spéciaux). Le FBI devrait-il être divisé en deux organismes, un pour l'application de la loi et l'autre pour le renseignement national?

Si le renseignement national constitue maintenant un besoin urgent, ne devrions-nous pas créer non seulement un Département de la sécurité intérieure, mais aussi un « Home Office » - l'équivalent du MI-5, le service de renseignement national britannique - comme plusieurs membres du Congrès l'ont proposé? La création d'un nouveau service ne réglerait pas les conflits découlant du chevauchement entre les missions - le MI-5 et le principal organisme d'application de la loi de la Grande-Bretagne, Scotland Yard, ont débattu pendant des années de la question de savoir qui s'occuperait en priorité de la menace terroriste que l'IRA représente pour l'Angleterre. Mais aux États-Unis, assez paradoxalement, les rapports hiérarchiques seraient peut-être plus clairs si un service distinct était créé pour le renseignement national, au lieu de réorganiser le FBI pour que le renseignement national y soit greffé.

À l'automne 2002, le Congrès a autorisé la création d'un nouveau département de la sécurité intérieure ayant sa propre section du renseignement. Cette section sera habilitée tant à recevoir des renseignements bruts qu'à assigner des tâches aux responsables de la collecte des renseignements. Elle devra avoir accès à des renseignements étrangers et aux informations sur des questions nationales provenant des organismes d'application de la loi. Ce ne sera pas simplement une section du renseignement comme l'INR du Département d'État. Elle devrait aussi servir l'ensemble des autorités, notamment à la Maison-Blanche, qui sont responsables de la sécurité intérieure.

Elle concentrera ses efforts sur le terrorisme et son mandat sera orienté en fonction des questions nationales. Parmi les institutions existantes, la CIA et le Counterterrorism Center, qui se trouve dans les locaux de la CIA, sont, pour des raisons légales, tournés principalement vers l'étranger. Ce sont les responsables des opérations, et non les analystes, qui dominent le centre. Avant la création du Département de la sécurité intérieure, étonnamment, aucun organisme n'examinait systématiquement les informations nationales à des fins de renseignement et d'alerte - par opposition à l'application de la loi; le FBI a seulement exprimé son intention de le faire.

La section du renseignement du Département de la sécurité intérieure devrait lier le renseignement plus étroitement aux avertissements. Après le bombardement de Pearl Harbor en 1941, on a craint de lier de trop près les avertissements aux opérations, mais il semble que ce soit la bonne façon de procéder maintenant. Dans la période qui a précédé le bombardement de Pearl Harbor, les services de renseignements de l'armée et de la marine avaient apparemment hésité à sonner le tocsin en se fondant sur des preuves inévitablement « douteuses ». Ils étaient proches de leurs collègues responsables des opérations et savaient donc que ce serait coûteux pour ces derniers de donner suite à un avertissement - prendre la mer, par exemple - si c'était une fausse alerte[3]. La préoccupation est légitime, mais maintenant ceux qui donnent l'alerte (à la CIA, par exemple) sont tellement éloignés de ceux qui doivent agir qu'ils sont tentés d'en faire trop - comme ce fut le cas à l'été 2002. Par ailleurs, la nouvelle section aura beaucoup de concurrence dans le milieu, ce qui suppose un grand nombre de vérifications si ses évaluations semblent être adaptées aux besoins des responsables des opérations du Département de la sécurité intérieure.

La nouvelle section pourrait aussi donner une raison de plus à la CIA et au FBI de communiquer entre eux. Elle constituerait une autre paire d'yeux qui examine les deux organismes et elle essaierait d'intégrer les informations provenant des deux. Cela contribuerait à peine à faciliter la communication entre ces deux grands organismes - le passé a laissé trop de traces, sans compter les préoccupations constitutionnelles. Mais la nouvelle section du renseignement serait un client ayant directement des intérêts dans le croisement des informations et des analyses produites par les deux.

Le Département de la sécurité intérieure a établi des cotes d'alerte nationale variant du vert au rouge, en passant par le bleu, le jaune et l'orange. L'idée est fondée sur vingt ans d'expérience en Grande-Bretagne. C'est une bonne idée, mais les États-Unis n'ont pas l'expérience de la Grande-Bretagne, de sorte que personne - ni l'État ni les autorités locales, encore moins les simples citoyens - ne sait

[3] L'étude classique de l'avertissement raté à Pearl Harbor est celle de Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford: Stanford University Press, 1962).

Partager avec « nous-mêmes »

Les distinctions n'ont pas été imposées aux États-Unis. Ce sont plutôt les Américains qui les ont choisies en grande partie, et le plus souvent pour de bonnes raisons. La CIA et le FBI étaient véritablement censés coopérer entre eux, mais pas *trop* étroitement, de crainte de violer les droits des Américains. L'ennui, c'est que la menace terroriste ne respecte aucune de ces distinctions. Elle chevauche l'ancien monde du renseignement et le nouveau. Elle fait partie de l'ancien monde parce que les terroristes n'annoncent quand même pas leurs plans, de sorte que les méthodes traditionnelles d'espionnage et d'écoute indiscrète sont essentielles. Mais elle fait aussi partie du nouveau monde, parce que même les États-Unis ne peuvent lutter seuls contre le terrorisme. Même si les États-Unis ont énormément amélioré le renseignement humain (HUMINT), d'autres pays et groupes - dont certains ne sont pas leurs alliés - réussiraient mieux qu'eux contre des cibles terroristes difficiles à surveiller. Les États-Unis ont révélé qu'ils partagent des renseignements avec 24 pays avec lesquels ils ne collaboraient pas avant la guerre actuelle. Cela comprend le Soudan, qui n'aurait été rien de plus qu'une cible avant le 11 septembre.

Le défi le plus dur est peut-être encore de coopérer avec « nous-mêmes » - entre les oppositions. Non seulement selon un rapport il existe aux États-Unis 18 000 entités gouvernementales participant à la guerre au terrorisme, mais s'ajoutent à cela de nombreux intervenants privés - des entreprises aussi bien que des ONG - et presque qu'aucun d'entre eux n'a d'autorisation de sécurité. Il n'est pas étonnant alors que le partage de renseignements jusqu'à présent ait été fait pas mal au hasard. Après le 11 septembre, des informations ont circulé à propos de menaces nucléaires pouvant peser sur New York, mais personne au gouvernement fédéral ne s'est donné la peine de communiquer cette information aux autorités new-yorkaises. À l'autre extrémité, le gouverneur de la Californie a jugé que des informations très partielles à propos de menaces visant les ponts dans cet État justifiaient une déclaration publique et il a augmenté la protection.

À l'instar du Canada, les États-Unis ont commencé à repenser les distinctions datant de la guerre froide. Les services de renseignements et les organismes d'application de la loi ont été poussés les uns vers les autres, mais la question de savoir jusqu'à quel point ils se sont rapprochés demeure controversée. Par exemple, depuis l'adoption de la *Patriot Act* aux États-Unis en 2001, il est plus facile de déplacer des informations entre les différentes structures. Avant l'adoption de la loi, toute information soumise à un grand jury fédéral pouvait être communiquée aux analystes de la CIA *seulement* avec une ordonnance de la cour. Des analystes pouvaient donc se voir refuser l'accès à des informations qui constituaient un morceau essentiel du casse-tête pour comprendre des réseaux terroristes. Maintenant, ces informations peuvent être partagées plus facilement. Cette loi a aussi allégé le critère sur lequel la FISC se fonde pour permettre des perquisitions secrètes si l'enquête sur de présumés liens avec l'étranger est un « motif secondaire ». La nouvelle loi a mis à jour le pouvoir de recourir à l'écoute électronique pour tenir compte du fait qu'il existe maintenant de multiples téléphones cellulaires mobiles, pas seulement des téléphones analogiques statiques. En 2002, Robert Mueller, directeur du FBI, a assoupli les règles qui empêchaient les agents du FBI de mener des activités auxquelles les simples citoyens peuvent se livrer, comme naviguer sur Internet ou visiter des églises ou autres lieux publics semblables présentant un intérêt.

Ces trois distinctions - entre application de la loi et renseignement, étranger et national, public et privé - étaient frappantes avant le 11 septembre. L'enquête du comité mixte de la Chambre et du Sénat sur les attentats du 11 septembre a fourni de nouveaux détails, mais l'histoire de base est restée la même[1]. Le partage d'informations entre les oppositions était, au mieux, inégal. Axée sur l'application de la loi et limitée par la nécessité d'ouvrir un dossier, la lutte du FBI contre le terrorisme était irrégulière. Bloqué par les grands murs protégeant la vie privée, le FBI a pu entrer dans l'ordinateur personnel de Zacarias Moussaoui, le présumé vingtième pirate de l'air, seulement après les attentats.

Par exemple, en août 2001, la CIA a apparemment envoyé un câble pour avertir que deux associés d'Oussama Ben Laden étaient entrés aux États-Unis et que deux autres devaient essayer de faire de même. Il semble que le FBI n'ait pas fait grand-chose avec l'information et que l'Immigration and Naturalization Service (INS) n'ait été mis au courant qu'après avoir admis au pays les deux autres, parce que l'INS n'était pas un organisme « d'application de la loi ». Aucun organisme n'a mis en garde la Federal Aviation Administration contre les quatre hommes, apparemment parce qu'elle non plus n'était pas un organisme d'application de la loi. Et personne n'a averti les compagnies aériennes parce qu'elles font partie du secteur privé et non du secteur public.

Dans l'intervalle, le présumé « vingtième pirate de l'air », Zacarias Moussaoui, avait été arrêté le 16 août à Minneapolis pour avoir enfreint les conditions de son visa. Les agents du FBI au bureau régional le soupçonnaient de terrorisme et essayaient, de plus en plus désespérément, d'entrer dans son ordinateur personnel. Ils étaient pris dans un débat avec l'administration centrale et le ministère de la Justice à propos de l'un de ces murs érigés entre le renseignement et l'application de la loi pendant les années 1970, la FISC. Avant la création de la FISC, les présidents revendiquaient le privilège d'effectuer des perquisitions sans mandat pour des raisons de sécurité nationale, de sorte que ce tribunal était un compromis entre la prérogative présidentielle et les libertés civiles. Avant le 11 septembre, cependant, selon les critères de la FISC, la « principale raison » justifiant une perquisition devait être un présumé lien avec une puissance étrangère, et Moussaoui, qui à ce moment là était associé seulement aux rebelles en Tchétchénie, ne répondait pas à ce critère[2].

[1] Voir http://www.fas.org/irp/congress/2002_rpt/index.html

[2] Philip Shenon, « Traces of Terror: The Terror Suspect », *New York Times,* 7 juillet 2002, p. A24.

La première opposition est celle entre l'application de la loi et le renseignement. Les deux domaines sont très différents. Le renseignement est orienté vers l'avenir et son but est d'informer les décideurs. Il vit dans un brouillard d'incertitude, où la « vérité » ne sera assurément jamais connue. Parce que les services de renseignements cherchent avant tout à protéger leurs sources et leurs méthodes, les responsables du renseignement veulent désespérément éviter de se retrouver dans la chaîne de possession des indices pour ne jamais avoir à témoigner en cour. De leur côté, les organismes d'application de la loi ne s'intéressent pas aux politiques. Ils s'occupent plutôt des poursuites judiciaires. Et ils savent que pour constituer un dossier, ils doivent être prêts à révéler des choses qui expliqueront comment ils en sont venus à savoir ce qu'ils savent.

La deuxième opposition est celle entre étranger et national. Lorsque le président Harry Truman a créé la CIA en 1946, il a exprimé ouvertement sa crainte de voir apparaître une « organisation semblable à la Gestapo », de sorte que le nouvel organisme a été exclu tant des activités ayant pour objet l'application de la loi que de celles liées aux questions nationales. Il est tout à fait vrai que dans les années 1970, les directeurs de la CIA et du FBI ne se parlaient pas. Les choses se sont améliorées, mais les relations entre les deux demeurent tendues. La National Security Agency est également exclue du domaine de l'application de la loi et des activités d'espionnage à l'intérieur du pays, de sorte que si les conversations privées qu'elle écoute présentent un intérêt « national » - elles se rapportent à un citoyen américain, à une entreprise américaine ou même à un étranger vivant au pays - l'écoute doit cesser.

Au milieu des années 1970, la première commission d'enquête sur le renseignement nommée par le Congrès (commission dont j'ai été membre), le comité sélect du Sénat chargé d'examiner les activités de renseignement, dirigé par Frank Church, alors sénateur de l'Idaho, a enquêté sur des cas de violation des droits des Américains. Les cas les plus graves, y compris le harcèlement de Martin Luther King et de nombreux groupes religieux et politiques américains, avaient été mis au jour par COINTELPRO, un curieux programme du FBI combinant l'application de la loi et le renseignement soi-disant aux fins du contre-espionnage national. Nous avons réagi en *élevant* des murs entre le renseignement et l'application de la loi - par exemple en créant une cour spéciale, la Federal Intelligence and Surveillance Court (FISC), pour l'examen des requêtes concernant la sécurité nationale, par opposition à l'application de la loi, l'écoute électronique et la surveillance.

La troisième est l'opposition entre public et privé. Pendant la guerre froide, la sécurité nationale était un monopole du gouvernement fédéral. Les simples citoyens et les entreprises étaient certes concernés, mais il y avait une nette relation entre la menace cernée et les mécanismes mis en branle par le gouvernement fédéral en matière de sécurité nationale pour faire face à cette menace. La guerre au terrorisme et la sécurité intérieure seront beaucoup moins un monopole du gouvernement fédéral. L'Américain moyen et l'économie souffrent déjà des inconvénients d'un resserrement des mesures de sécurité et de l'augmentation des coûts que celles-ci supposent pour le milieu des affaires. Et, tragiquement, un plus grand nombre d'Américains ordinaires sont susceptibles d'être tués - entraînés involontairement dans la guerre au terrorisme.

Aujourd'hui, les casse-têtes tactiques où les secrets ont de l'importance sont à la fois moins nombreux et plus variés qu'à l'époque de la guerre froide, mais ils demeurent importants. Pour résoudre les casse-têtes, les analystes doivent être proches de ceux qui recueillent les secrets. Dans un monde caractérisé par une surabondance d'informations, les décideurs voudront aller chercher ce dont ils ont besoin et non se faire imposer des informations; ils voudront aller chercher des solutions aux casse-têtes lorsqu'ils en auront besoin, plutôt que de recevoir un torrent d'informations, qu'ils l'aient demandé ou non. Il n'en demeure pas moins que la résolution du casse-tête est souvent suffisamment importante pour qu'il ne soit aucunement difficile d'amener les décideurs à prêter attention.

Les mystères, comme la question de savoir où et comment les terroristes attaqueront la prochaine fois, abondent certainement plus de nos jours, et la clarification de mystères stratégiques est un domaine très différent de celui de la résolution de casse-têtes. Pour élucider des mystères, les analystes doivent avoir accès à des secrets, mais leurs partenaires essentiels sont des collègues à l'extérieur des services de renseignements et du gouvernement, ou des collègues du milieu universitaire, des groupes de réflexion, des organisations non gouvernementales (ONG) et du milieu des affaires. Le renseignement doit être grand ouvert, et non enfermé dans des compartiments secrets. Dans ce domaine, il faut partir du principe que les services de renseignements s'occupent d'informations, et non de secrets, et qu'ils travaillent avec des gens (des spécialistes), et non des documents.

Dans un monde où le contrôle tant des structures que des intérêts américains est laissé à tout un chacun, les décideurs seraient peut-être mieux servis par des courtiers en renseignement se trouvant à proximité - au bout du couloir, non pas à la CIA en Virginie. Une autre des distinctions prévalant pendant la guerre froide devrait alors s'estomper, soit celle entre les politiques et les renseignements. Il existe certains parallélismes constants entre les cibles, les analystes, les clients et ceux qui recueillent les renseignements. Dans de telles circonstances, une entreprise s'organiserait autour d'un secteur d'activité, établissant un réseau réparti ou une confédération plus ou moins structurée dans laquelle différentes parties des services de renseignements essaieraient d'établir des liens très étroits avec leurs clients respectifs. Les centres existants relevant du directeur des services centraux du renseignement (DCI) - pour la lutte contre le terrorisme, la lutte contre le trafic de drogue et autres - constituent un modèle évocateur. Ils s'organisent autour d'un problème ou d'une politique. Leurs limites tiennent au fait qu'ils travaillent principalement *à l'intérieur* du monde du renseignement, bien que les liens avec le secteur des politiques s'établissent par leur intermédiaire. Et le réseau réparti serait « virtuel », parce que s'il est vrai que certains problèmes, comme dans le cas de la Corée du Nord ou du terrorisme, persisteront, d'autres surgiront et disparaîtront rapidement.

La force des « oppositions » de la guerre froide

Le legs de la guerre froide ne se limite pas à des distinctions entre les secrets et les informations de sources ouvertes, les analystes et les responsables de la collecte, les politiques et les renseignements. Pour de bonnes raisons, la plupart liées à la protection des droits des citoyens, les États-Unis ont créé des « oppositions » qui n'étaient pas mauvaises pendant la guerre froide, mais qui nous vouent à l'échec dans la guerre actuelle contre le terrorisme.

la notion de cloisonnement) pouvaient chacun se concentrer sur leur façon particulière de contribuer à faire la lumière sur la cible dominante, l'Union soviétique. En cours de route, cependant, les services de renseignements sont devenus à proprement parler de redoutables baronnies. Parallèlement, l'analyse était centralisée à la Direction du renseignement (DI) de la CIA, qui toutefois n'en avait pas le monopole; la DI avait des concurrents à la Defense Intelligence Agency (DIA), au Bureau of Intelligence and Research (INR) du Département d'État et ailleurs dans les hautes sphères de Washington.

Cependant, l'ancienne structure ne peut tout simplement plus convenir. Aucune organisation ne fonctionnerait de cette manière; les choses ont tellement changé! Pendant la guerre froide, il y avait une seule cible dominante, l'Union soviétique, un ensemble assez restreint de clients - surtout des représentants politiques et militaires du gouvernement américain - et une quantité limitée d'informations, la plupart provenant de sources spéciales qui « appartenaient » à des services de renseignements et étaient jugées fiables. Dans le nouveau contexte, toutefois, les cibles et les clients sont nombreux, et les informations circulent abondamment, la plupart n'« appartenant » pas à des services de renseignements et leur degré de fiabilité variant beaucoup, comme n'importe quel internaute peut en témoigner.

L'explosion d'informations signifie que les décideurs dépendront davantage, et non moins, des courtiers en information. Si la collecte est plus facile, la *sélection* sera plus difficile. Parce que le monde est plus ouvert, la distinction entre collecte et analyse, comme à l'époque de la guerre froide, est de moins en moins nette. Le meilleur informateur n'est pas un maître de l'espionnage, encore moins un satellite impersonnel, mais quelqu'un plongé dans la matière disponible - bref, un analyste. Néanmoins, les analystes sont reconnus comme étant des généralistes, et non de grands spécialistes, et dans certains domaines comme l'économie, les services de renseignements ne peuvent rivaliser avec le secteur privé. Cependant, les analystes sont bon marché comparativement à des satellites, et l'embauche d'un plus grand nombre de gens de l'extérieur, même pour de brèves affectations, renforcerait le savoir-faire de la communauté du renseignement.

Les casse-têtes par opposition aux mystères

De nos jours, le renseignement fait partie du monde de l'information, pas seulement le monde des secrets, ce qui constitue un profond changement pour la profession. À l'ère de l'information, le moment est venu pour la communauté du renseignement de « diviser le domaine » en casse-têtes et mystères. Il existe des solutions précises aux casse-têtes, si seulement nous avions accès aux informations nécessaires (secrètes). Les casse-têtes étaient les outils de la communauté du renseignement pendant la guerre froide. Combien de missiles l'Union soviétique possède-t-elle? Quel est leur degré de précision? Quel est l'ordre de bataille de l'Irak? Les « mystères » sont à l'opposé des casse-têtes; ce sont des questions auxquelles il n'existe pas de réponse définitive, même en principe. La Corée du Nord concluera-t-elle une nouvelle affaire nucléaire? Le Parti communiste chinois abandonnera-t-il sa primauté nationale? Quand et où Al Qaida attaquera-t-il la prochaine fois? Personne ne connaît les réponses à ces questions. Le mystère ne peut être qu'éclairci; il ne peut être « résolu ».

Introduction

Le monde du renseignement commençait tout juste à s'acclimater à la fin de la guerre froide lorsque les attentats terroristes du 11 septembre ont eu lieu. La chute de l'Union soviétique a éliminé la menace qui servait de point de repère pour évaluer tout le reste. Parallèlement, la distinction entre le renseignement stratégique et le renseignement tactique s'est estompée en raison de l'évolution rapide de la technologie, et l'explosion de réseaux d'information mondiaux a créé des occasions pour les services de renseignements nationaux et les a mis en concurrence les uns avec les autres. Avec l'effondrement de l'Union soviétique et la diminution du nombre de régions dans le monde auxquelles il est impossible d'avoir accès, sans compter la révolution technologique, les services de renseignements ont commencé à apprendre à traiter d'énormes quantités d'informations de sources ouvertes, mais où s'entremêlent les faits, la fiction, la fantaisie et la désinformation.

Puis il y a eu les attaques du 11 septembre. La menace qui pointait à l'horizon n'est devenue que trop réelle, et soudain une intervention immédiate des services de renseignements s'imposait, pas seulement aux différents paliers des systèmes fédéraux. Aux fins de cette intervention, il fallait aussi passer outre à des distinctions - application de la loi et renseignement, national et étranger, public et privé - qui étaient déjà remises en question. Ce genre d'intervention est peut-être la plus difficile de toutes, car elle oblige les services de renseignements de tous les pays non seulement à partager des informations entre eux, mais à travailler chez eux avec divers représentants gouvernementaux et simples citoyens, qui sont de nouveaux venus dans le domaine du renseignement et découvrent ce qu'est le renseignement et ce qu'il peut faire ou non.

De par leur grosseur et leur technologie, les services de renseignements américains sont dans une classe à part. Il est néanmoins frappant de constater jusqu'à quel point les pays qui prenaient le renseignement au sérieux pendant la guerre froide ont tous le même défi à relever - que ces pays aient été neutres auparavant ou qu'ils soient des alliés de l'OTAN ou d'anciens ennemis. Tous ont des institutions importantes responsables du renseignement, qui en grande partie étaient dominées par l'armée. Tous se demandent comment cette capacité peut être remodelée en fonction d'un nouveau monde et de nouvelles menaces, et ce, sans trop empiéter sur les libertés de leurs citoyens. En ce sens, l'exemple des États-Unis peut être instructif, tout comme les États-Unis peuvent de leur côté tirer profit des expériences des autres.

Le legs de la guerre froide

Pendant la guerre froide, il y avait une certaine logique dans la façon dont les services de renseignements américains étaient organisés. Ils étaient structurés en fonction des *sources,* c'est-à-dire selon les différentes manières dont les renseignements sont recueillis : la National Security Agency (NSA) pour l'interception des signaux ou SIGINT; le service clandestin de la CIA pour l'espionnage ou le renseignement humain (HUMINT); et la National Imagery and Mapping Agency (NIMA), créée récemment, pour l'imagerie ou IMINT. (Dans le jargon du renseignement, tout ce qui ne provient pas d'une source secrète est une « source ouverte ».) Ces différents services de renseignements (dans le jargon du métier, les anglophones les appellent « stovepipes » pour exprimer

Non classifié
Été 2003
N° 82

Service canadien du renseignement de sécurité

Commentaire

Remodeler le renseignement pour le partager avec « nous-mêmes »

Gregory F. Treverton